Tailoring zero trust to **individual users**

By understanding normal behavior, agencies can develop more granular cybersecurity strategies and control

Sean Berg
President of Global Governments and Critical Infrastructure, Forcepoint

IT INFRASTRUCTURES HAVE CHANGED substantively due to the remote workforce, digital transformation, the march to the cloud and the need to share information across agencies. When everything was behind a firewall, agencies could protect the network adequately. But now data is everywhere, so agencies have to take a different approach to security.

Zero trust is an important construct for helping agencies protect their infrastructure in today's cybersecurity landscape. It focuses on accrediting individuals and their access to government resources. Agencies should make those decisions about access based on a comprehensive understanding of users.

Security policies that treat all users as equally risky can be restrictive. Such policies set the bar high and hamper employees' ability to work, or they set the bar low, which defeats the purpose of having security.

Instead, agencies should evaluate users on an individual basis by taking the time to understand what employees do and how they do it — what's normal behavior and what's not. Then they can assess the risk of an individual based on that context.

Applying the appropriate level of security

Agencies should pay attention to how employees interact with data and other resources as well as how they interact with the identity, credential and access management (ICAM) system. IT administrators can use analytics to understand that behavior and then apply the appropriate level of security.

For high-risk individuals, administrators may want to change the ICAM policy associated with them. Perhaps they should be required to use multifactor authentication every hour to ensure their credentials haven't been compromised, while less-risky users would only have to authenticate their identities once or twice a day.

Tools that monitor behavior are also adept at identifying potential insider threats. They simplify the validation of whether an activity had malicious intent or whether someone made a mistake because they weren't trained correctly.

In addition, just as these risk scoring and response tools are tailored to individual users, a zero trust strategy must also be adapted to the unique needs of the organization. For example, the intelligence community's approach would be very different from that of a civilian agency or a critical infrastructure provider.

The limits of threat-based cybersecurity

At Forcepoint, we focus on building adaptive and context-based zero trust architectures, and we've made two acquisitions this year to strengthen our support of agencies' cybersecurity efforts.

Shutterstock/FCW Staff

> **A zero trust architecture assumes everything is potentially risky** to ensure that agencies can deal with emerging threats and continue to evolve their cybersecurity strategies.

We added Cyberinc and its technology for remote browser isolation. Rather than allow an employee to visit a potentially malicious website, an agency can spin up a virtual container behind the scenes that accesses the site and relays it to the user. The employee's device — and by extension, the government network — stays safe while also enabling IT control.

We also acquired U.K.-based Deep Secure. The company's government defense-grade technology will allow Forcepoint to extend the capabilities of our cross-domain solutions for securing mission-critical data. In addition, Deep Secure's Threat Removal platform is a content disarm and reconstruction technology that deconstructs files and rebuilds them to eliminate anything malicious embedded in those files.

It is important to remember that threat-based cybersecurity is vulnerable to zero-day attacks, which exploit previously unknown vulnerabilities. By contrast, a zero trust architecture assumes everything is potentially risky to ensure that agencies can deal with emerging threats and continue to evolve their cybersecurity strategies. ■

Sean Berg is president of global governments and critical infrastructure at Forcepoint.